

What is claimed is:

- 1 1. A method of dynamically protecting access to a first network, comprising:
2 receiving, in a system, a data unit containing a source address indicating a
3 source of a data unit;
4 matching the source address with information stored in the system; and
5 enabling entry of the data unit to the first network if the source address
6 matches the information stored in the system and denying entry of the data unit to the
7 first network if the source address does not match the information stored in the system.

- 1 2. The method of claim 1, wherein matching the source address with the
2 information comprises matching the source address with one or more entries of a network
3 address translation mapping table.

- 1 3. The method of claim 1, wherein matching the source address comprises
2 matching an Internet Protocol address.

- 1 4. The method of claim 1, wherein receiving the data unit comprises
2 receiving a data unit containing media associated with a call session.

- 1 5. The method of claim 1, further comprising determining if the data unit
2 contains a payload according to a predetermined protocol, and denying entry of the data
3 unit if the data unit does not contain payload according to the predetermined protocol.

- 1 6. The method of claim 5, wherein determining if the data unit contains a
2 payload according to the predetermined protocol comprises determining if the data unit
3 contains a payload according to a Real-Time Protocol or Real-Time Control Protocol.

- 1 7. The method of claim 1, further comprising storing profile information for
2 each call session, and determining if an unauthorized access of the first network is
3 occurring based on the profile information.

1 8. The method of claim 7, wherein storing the profile information comprises
2 storing a threshold representing a maximum acceptable rate of incoming data units from
3 an external network to the first network.

1 9. The method of claim 8, further comprising calculating a value for the
2 threshold based on a frame size used in the call session.

1 10. The method of claim 8, wherein storing the profile information further
2 comprises storing a pattern expected in incoming data units.

1 11. The method of claim 10, wherein storing the pattern comprises storing a
2 codec type used in the call session.

1 12. The method of claim 8, further comprising generating an alarm if the
2 system detects a rate of incoming data units from the external network to the first
3 network exceeding the threshold.

1 13. The method of claim 8, further comprising denying further transport of
2 incoming data units from the external network to the first network for the call session if
3 the system detects a rate of incoming data units from the external network to the first
4 network exceeding the threshold.

1 14. An article comprising at least one storage medium containing instructions
2 for protecting a first network, the instructions when executed causing a system to:
3 determine if a rate of incoming data units from an external network to the
4 first network exceeds a predetermined threshold; and
5 perform a security action if the determined rate of incoming data units
6 exceeds the predetermined threshold.

1 15. The article of claim 14, wherein the instructions when executed cause the
2 system to determine if the rate of incoming data units exceeds the predetermined
3 threshold in a given call session.

1 16. The article of claim 15, wherein the instructions when executed cause the
2 system to further store plural thresholds for corresponding plural call sessions.

1 17. The article of claim 15, wherein the instructions when executed cause the
2 system to further calculate the predetermined threshold based at least in part on a frame
3 size used in the call session.

1 18. The article of claim 14, wherein the instructions when executed cause the
2 system to further determine if each incoming packet has a predetermined pattern.

1 19. The article of claim 18, wherein the instructions when executed cause the
2 system to determine if each incoming packet has the predetermined pattern by checking if
3 each incoming packet has an indication of a predetermined codec type.

1 20. A system for use in communications between a first network and an
2 external network, comprising:

3 a storage module to store a threshold value for a communications session,
4 the threshold value representing an acceptable rate of incoming data units from the
5 external network to the first network; and

6 a controller adapted to deny further entry of data units from the external
7 network to the first network in the communications session in response to the controller
8 detecting that the rate of incoming data units exceeds the threshold value.

1 21. The system of claim 20, the storage module to further store address
2 information, wherein the controller is adapted to compare a source address of an
3 incoming data unit with the address information stored in the system and to deny further
4 entry of the incoming data unit if the source address does not match the address
5 information stored in the system.

1 22. The system of claim 21, wherein the address information comprises a
2 network address translation table.

1 23. The system of claim 22, wherein the network address translation table
2 comprises a network address and port translation table.

1 24. The system of claim 21, wherein the controller is adapted to further check
2 if the incoming data unit contains a Real-Time Protocol or Real-Time Control Protocol
3 payload, and to deny further entry of the incoming data unit if the incoming data unit
4 does not contain a Real-Time Protocol or Real-Time Control Protocol payload.

1 25. The system of claim 20, the storage module to further store a codec type
2 for the communications session, wherein the controller is adapted to deny entry of an
3 incoming data unit if the incoming data unit does not contain an indication of the codec
4 type.

SEARCHED
INDEXED
SERIALIZED
FILED